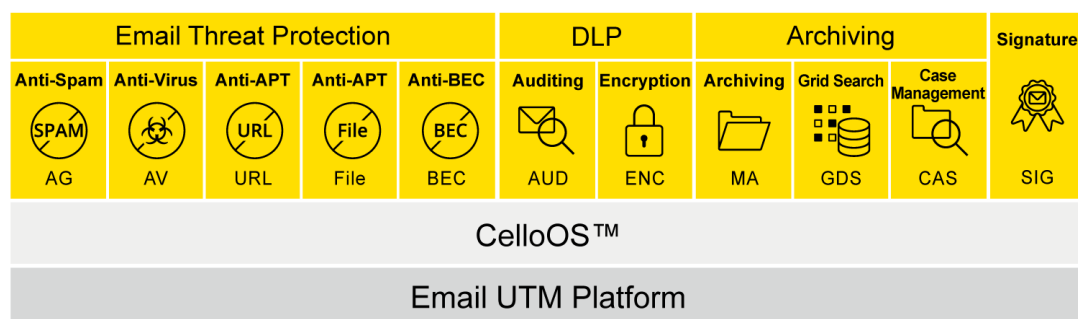**CELLOPOINT**
Secure Your Email

Work smart with Email UTM.
Simple, flexible and high
efficacy.

Email UTM

Cellopont Email UTM (Unified Threat Management) is an email gateway deployed in front of the email server. Powered by CelloOS, it allows flexible integration of Inbound email security, Archiving, and Outbound Email DLP modules, all within the same operating system. By using Cellopoint Email UTM platform, organizations can enhance their email security and risk management, ultimately lowering total operational costs.

Email Threat Protection					DLP		Archiving			Signature
Anti-Spam	Anti-Virus	Anti-APT	Anti-APT	Anti-BEC	Auditing	Encryption	Archiving	Grid Search	Case Management	
SPAM		URL	File	BEC						
AG	AV	URL	File	BEC	AUD	ENC	MA	GDS	CAS	SIG

CelloOS™

Email UTM Platform

UTM Features

Industry Leading CelloOS™

CelloOS™ is an advanced operating system built to optimize email security and performance, featuring MTA, system monitoring, incident logs, and reports. With the CelloOS™ flexible platform, organizations can select and activate optional security and risk management modules to suit their needs.

Five Layered Inbound Email Security:

Anti-Spam: With dynamic Sender Reputation List (SRL), Anti-Spam rule, and real-time updates from Cellopoint Global Anti-Spam Center, spam and unsolicited ads emails are effectively blocked.

Anti-Virus: Uses multilayered antivirus engines such as ClamAV, Bitdefender (Optional), and provides online virus pattern updates, effectively blocking known threats such as viruses, worms, spyware, trojans, ransomware, and other malware.

Anti-APT-URL : Detects carefully crafted phishing emails by analyzing phishing URLs and malicious links, with additional Time of Click (ToC) detection for an extra layer of protection.

Anti-APT-File: Detects the latest targeted attacks by performing sandbox analysis on attachments. It utilizes detonation analysis to identify unknown malicious programs and ransomware that have not yet been updated with virus signatures.

Anti-BEC: Targets Business Email Compromise (BEC) scams by detecting sender impersonation and abnormal email activity and alerting recipients to prevent them from being tricked into transferring funds or sharing confidential information.

Features

- Anti-spam detection
- Anti-virus detection
- Anti-APT-URL detection
- Anti-APT-File detection
- Anti-BEC scam detection
- Email archiving and retrieving
- Email auditing
- Email Encryption
- Digital Signature

Benefits

- Increases employee productivity
- Enhances email server performance
- Saves IT staff time
- Controls email traffic
- Offers flexible management for individuals and group
- Regulatory compliance
- Email Lifecycle Management
- Secures email transmission
- Reduces total cost of ownership (TOC)

Archiving Modules

Mail Archiving：Conducts fingerprinting, timestamping, indexing, compression, and encryption on inbound, outbound, and local (internal) emails, enabling automatic archiving, digital evidence preservation, and Email Lifecycle Management (ELM) for quick searching and retrieval.

Grid Search：Manages and retrieves large volumes of archived email data by distributing the indexing of archived emails to multiple Grid Search Accelerators (GSA), providing an industry-leading high-speed retrieval framework.

Case Management：Creates groups, assigns relevant emails for analysis, manages case assignments, assists legal teams with digital evidence, and reduces operational risks.

Outbound Email DLP Modules

Auditing: Set email content audit policies and use real-time scanning engines to audit sensitive emails, preventing the leakage of sensitive information.

Encryption：Automatically encrypts outbound emails using a flexible policy engine, supporting TLS, HTTPS, S/MIME, and PDF to ensure secure transmission.

Digital Signature: Automatically applies digital signatures at the gateway to prevent email spoofing, ensuring the integrity and non-repudiation of outbound emails.

Highlights

- Web-based console for easy email policy setup
- Integrates with POP3, LDAP, Active Directory, and on-premises authentication
- Web-based reportin with multiple export options (Word, Excel, HTML)
- Supports syslog and CEF logging for SIEM integration
- Single-node and multi-node Active-Active clustering
- Scalable console, scanners, and storage
- Compatible with x86 servers and virtualization platforms
- Supports VMware, Hyper-V, and XenServe
- Integrates with cloud platforms (Azure, AWS, GCP)

Supported Email Systems

- Microsoft Exchange 2016 / 2019 / 2022/ Microsoft 365 / Exchange Online
- Google Workspace
- Zimbra
- HCL Notes
- Sendmail / Qmail / Postfix

Specifications

CelloOS	SEG	AG	Anti-spam provides anti-spam rule updates and online defense.
		AV	AV engines provide virus scanning and online virus pattern updates.
		URL	Anti-APT-URL provides phishing & malicious URL detection, real-time TI updates, and ToC detection.
		File	Anti-APT-File provides unknown malware detection with sandbox emulation, correlation analysis, and real-time TI updates (Optional On-premises sandbox)
		BEC	User behavior modeling, sender impersonation detection, and abnormal email alerts and management.
	MA	MA	Mail Archiving provides archiving and backup with indexing
		GDS	Grid search provides distributed indexing with cloud computing techniques.
		CAS	Case Management provides archived email categorization and audit flow.
	DLP	AUD	Auditing provides policy-based email filtering and auditing.
		ENC	Encryption provides outbound email encryption.
	SIG		Digital Signature provides automatic digital signature inclusion.

※All the modules above include an initial fee for first-year license access, followed by yearly maintenance fees.
※The number of licenses is according to the number of email accounts.